

INTERNET DOCUMENT INFORMATION FORM

**A . Report Title: SOHO MISSION INTERRUPTION JOINT
NASA/ESA INVESTIGATION BOARD**

B. DATE Report Downloaded From the Internet: OCT 13 98

**Report's Point of Contact: (Name, Organization, Address, Office
Symbol, & Ph #): NASA WASHINGTON, DC**

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

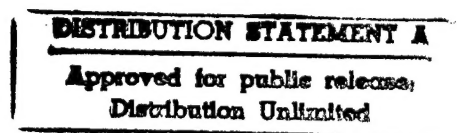
**F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __LL__ Preparation Date 15 OCT 98**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.

AQ 499-01-0061

**SOHO Mission Interruption Joint NASA/ESA
Investigation Board**

Final Report



19981019 033

**August 31, 1998
SOHO Mission Interruption Joint NASA/ESA
Investigation Board**

Prof. Massimo Trella, Co-Chairperson
Inspector General, ESA

Dr. Michael Greenfield, Co-Chairperson
Deputy Associate Administrator,
Office of Safety and Mission Assurance
NASA/Headquarters

Ellen L. Herring, Executive Secretary
Office of Systems Safety and Mission Assurance
NASA's Goddard Space Flight Center

John Credland
Head, Science Projects Department
ESA/ESTEC

Dr. H. Richard Freeman
Chief Engineer,
Applied Engineering and Technology Directorate
NASA's Goddard Space Flight Center

Robert Laine
ESA XMM Project Manager
ESA/ESTEC

William Kilpatrick
Chief, Systems Engineering Laboratory
NASA's Marshall Space Flight Center

Dino Machi
Project Manager, International Flight Projects
NASA's Goddard Space Flight Center

Alan Reth
Guidance Navigation, and Control Center
Applied Engineering and Technology Directorate
NASA's Goddard Space Flight Center

Alan Smith
Head, Flight Operations Division
ESA/ESOC

SOHO MISSION INTERRUPTION JOINT ESA/NASA INVESTIGATION

BOARD REPORT

TABLE OF CONTENTS

TOPIC PAGE

EXECUTIVE SUMMARY 1

INTRODUCTION 2

BACKGROUND 3

FACTORS DIRECTLY CONTRIBUTING TO THE LOSS 6

FACTORS INDIRECTLY CONTRIBUTING TO THE LOSS 8

Ground Procedures

Procedure Implementation

Management Structure and Process

Ground Systems

RECOMMENDATIONS 14

Ground Procedures

Procedure Implementation

Management Structure and Process

Ground Systems

APPENDICES

APPENDIX A. Assignment Letter

APPENDIX B. Summary of Interviewed Individuals

APPENDIX C. Sequence of Events

APPENDIX D. Failure Event Tree

APPENDIX E. A_CONFIG_N Modification History

ACRONYM LIST

EXECUTIVE SUMMARY

Contact with the SOLar Heliospheric Observatory (SOHO) spacecraft was lost in the early morning hours of June 25, 1998, Eastern Daylight Time (EDT), during a planned period of calibrations, maneuvers, and spacecraft reconfigurations. Prior to this the SOHO operations team had concluded two years of extremely successful science operations. A joint European Space Agency (ESA)/National Aeronautics and Space Administration (NASA) engineering team has been planning and executing recovery efforts since loss of contact with some success to date.

ESA and NASA management established the SOHO Mission Interruption Joint Investigation Board to determine the actual or probable cause(s) of the SOHO spacecraft mishap.

The Board has concluded that there were no anomalies on-board the SOHO spacecraft but that a number of ground errors led to the major loss of attitude experienced by the spacecraft.

The Board finds that the loss of the SOHO spacecraft was a direct result of operational errors, a failure to adequately monitor spacecraft status, and an erroneous decision which disabled part of the on-board autonomous failure detection. Further, following the occurrence of the emergency situation, the Board finds that insufficient time was taken by the operations team to fully assess the spacecraft status prior to initiating recovery operations. The Board discovered that a number of factors contributed to the circumstances that allowed the direct causes to occur.

The Board strongly recommends that the two Agencies proceed immediately with a comprehensive review of SOHO operations addressing issues in the ground procedures, procedure implementation, management structure and process, and ground systems. This review process should be completed and process improvements initiated prior to the resumption of SOHO normal operations.

-

-

INTRODUCTION

The SOHO mission is a prime component of the joint ESA/NASA International Solar Terrestrial Program (ISTP). ESA was assigned the responsibilities for the spacecraft procurement and spacecraft final integration and test. NASA was assigned the responsibilities for the launcher, launch services, and the ground segment system to support pre-launch activities and in-flight operations. The SOHO spacecraft was built in Europe by an industrial team led by Matra Marconi Space (MMS) with instruments provided by nine European and three American Principal Investigators (PI's). SOHO was launched on December 2, 1995. The SOHO mission operations are provided by NASA under a Goddard Space Flight Center (GSFC) contract with the Allied-Signal Technical Services Corporation (ATSC). Following

spacecraft checkout and the transition from low earth orbit into a halo orbit around the Lagrangian L1 point of the Sun-Earth system, the SOHO mission was declared fully operational in April 1996. SOHO has completed its two year primary mission and entered into its extended mission phase in May 1998.

Distinctive SOHO discoveries have been realized in the areas of helioseismology, solar atmosphere and corona, and solar wind. Highlights of these discoveries include the first ever image of the convection zone of a star, the first ever tracing of the slow speed solar wind near the equatorial current sheet, and the detection of elements and isotopes never seen before in the solar wind, along with higher time resolution than ever before possible in solar wind composition. Additional information on SOHO scientific findings are maintained on and accessible to the global outreach community through the World Wide Web at URLs <http://sohowww.nascom.nasa.gov/> and <http://sohowww.estec.esa.nl/>.

Contact with the SOHO spacecraft was lost in the early morning hours of June 25, 1998, EDT, during a planned period of calibrations, maneuvers, and spacecraft reconfigurations. A joint ESA/NASA engineering team has been planning and executing recovery efforts since loss of contact with some success to date.

ESA and NASA management established the SOHO Mission Interruption Joint ESA/NASA Investigation Board to determine the actual or probable cause(s) of the SOHO spacecraft mishap. The Board was asked to focus on the discovery of root cause-effect relationships from which remedial and corrective actions can be derived. Due to the programmatic, technical, and operational complexities of this mission, the intent of the investigation was to determine how processes and responsibilities may be clarified and improved. The Board was directed to provide all pertinent information concerning the incident, along with recommended preventive measures to preclude similar mishaps on other missions, in a final report to the ESA Director of Scientific Programme and to the NASA Associate Administrator of the Office of Space Science. An interim report was provided on July 10, 1998 outlining primary causes and recovery options. The Assignment Letter establishing the Board and identifying its responsibilities, membership, and initial operating mandate is provided in Appendix A.

Representation on the Board reflected the international aspect of the SOHO mission and the desire to independently assess the mishap from a total system perspective. The Board was co-chaired by Professor Massimo Trella, ESA Inspector General, and Dr. Michael A. Greenfield, NASA Deputy Associate Administrator, Office of Safety and Mission Assurance. The Board membership consisted of ESA and NASA managers and engineers with broad experience in both the development and operations of flight projects.

The Board began the investigation process by reviewing the SOHO mission goals, the spacecraft design and implementation, the management roles and responsibilities, and the mishap sequence of events. Following this high level familiarization process, the Board interviewed persons believed to have had a substantial involvement in the events that may have led to the mishap. A summary of personnel interviewed is provided in Appendix B. These individual interviews were aimed at both understanding the facts as they occurred and at understanding the individual perceptions that may have been instrumental in the decisions and judgments that were made. Action items were identified and assigned throughout the process and the action item responses as well as SOHO mission documentation were analyzed as part of the final analytical process.

The Board wishes to acknowledge the contributions of all those who supported the education and interview process. All persons interviewed were open, forthright, and professional.

-

BACKGROUND

SPACECRAFT CONTROL

The incident was preceded by a routine calibration of the spacecraft's three roll gyroscopes (gyros) and by a momentum management maneuver. The spacecraft roll axis is normally pointed toward the Sun and the three gyros are all aligned to measure incremental changes in the spacecraft roll attitude.

Gyro calibrations are performed to accurately determine the drift bias that is associated with each of the three roll axis gyros. The electrical drift bias is the rate output value that a gyro exhibits when the spacecraft has absolutely no angular rotational motion about its roll axis. Once these biases are accurately determined, the bias values are uplinked to the spacecraft computer to be subtracted from the gyro measurements (to determine the actual motion of the spacecraft). Drift biases change slowly over time and temperature; consequently, gyro calibrations must be performed periodically so that the attitude control system can meet its pointing requirements.

The gyros are not required during most of the mission. They are used for thruster-based activities such as momentum management, Emergency Sun Reacquisition (ESR), and Initial Sun Acquisition (ISA).

Momentum management is accomplished using the spacecraft's Attitude Control Unit (ACU) computer, and is performed approximately every 2 months to maintain the reaction wheel speeds within prescribed limits. Reaction wheels provide control torques to control spacecraft attitude. Control torques are needed in order to counteract internal and external disturbance torques imparted to the spacecraft, and to slew the spacecraft for special off-pointing and roll-offset maneuvers.

Momentum management is necessary because the reaction wheels increase in speed over time in order to maintain spacecraft attitude in the presence of external disturbance torques. As the wheels accelerate to speeds that approach their design limit, momentum management is performed to reset the reaction wheel speeds to nominal values.

In the momentum management mode, the ACU computer despins the wheels and controls the attitude of the spacecraft using thrusters. The attitude disturbance that would be otherwise caused by the wheel deceleration is counteracted by the firing of the thrusters.

The ESR mode is a "Safe Hold Mode" or a "safety net" configuration autonomously entered by the spacecraft in the event of anomalies. ESR is a hardwired, analog control mode that is part of the Fault Detection Electronics (FDE). Unlike the other control modes, it is not operated under the control of the ACU computer. Thrusters are used in ESR to control the spacecraft.

Once the spacecraft has entered the ESR mode, a recovery sequence must be commanded and executed under ground operator control to proceed to the Mission Mode, the mode from which science observations are made. The first step along this recovery sequence involves the use of the ISA mode, a mode in which the ACU computer fires spacecraft thrusters to point the spacecraft toward the Sun under the guidance of an onboard Sun-sensor.

Normally, the 3 roll gyros perform the following functions:

Gyro A - connected to FDE for roll rate sensing for ESR using thrusters.

Gyro B - connected to FDE for excessive roll rate (anomaly) detection

Gyro C - connected to ACU for roll attitude sensing during computer-based control modes using thrusters

Conservative gyro usage had been planned because gyros are recognized to be life limited items. Problems encountered in other programs using similar gyros led to introduction of additional changes following launch to further preserve gyro lifetime. Consequently, Gyro A was deactivated (spun down) after a calibration maneuver to conserve its life. There is an automatic on-board function to respin Gyro A if the spacecraft autonomously enters its ESR mode. However all gyros are intended to be fully active during momentum management maneuvers.

OPERATIONAL TIMELINE

There are many operational procedures such as momentum management, gyro calibration, and science instrument calibration that are required for the execution of the SOHO mission that are grouped to minimize the impact on science downtime.

Previously these groups had been conducted in discrete blocks each executed during one 12-hour day shift. The difference with the events leading to this incident was that the operation had been compressed into a continuous sequence. This required a new script and first time utilization of paths within previously modified procedures.

FACTORS DIRECTLY CONTRIBUTING TO THE LOSS

The Board has concluded that there were no anomalies on-board the SOHO spacecraft but that a number of ground errors led to the major loss of attitude experienced by the spacecraft.

The first two errors were contained in predefined command sequences executed from the Ground System, while the last error was a decision to send a command to the spacecraft in response to unexpected telemetry. The sequence of these errors and their relationship to the triggered-ESRs are graphically depicted in Diagram 1.

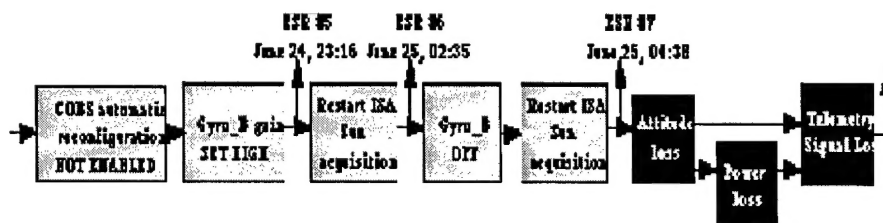


Diagram 1. Failure Event Tree - Top Level

This series of events was preceded by a routine calibration of the spacecraft's three roll gyros. As stated earlier, the gyros are not required during most of the mission. They are used for thruster-based activities such as momentum management, ISA, and ESR.

Since the gyro calibration in the compressed timeline is immediately followed by the execution of momentum management, the previously employed procedure to despin the gyros at the end of the gyro calibration and to re-enable the on-board software gyro control function was not required. Following gyro calibration, Gyro A was specifically deactivated (despun) in order to conserve its life, while Gyros B and C remained fully active. Due to an omission in the modified predefined command sequence actually used, the onboard software function that activates the gyro needed by ESR was not enabled. **This omission resulted in the removal of the functionality of the normal safe mode and ultimately caused the catastrophic sequence of events.**

Following the momentum management maneuver, Gyro B, which is used for fault detection, was erroneously left in its high gain setting, resulting in an indicated roll rate of 20 times greater than actual. **The incorrect gain was due to an error in another predefined command sequence; this error resulted in an on-board fault detection output that triggered an ESR.** This ESR, the 5th since launch, occurred at 7:16 PM EDT (23:16 UT), June 24, 1998.

During ESR-5, the control Gyro A was not active because of the first error referenced above; however, there is no evidence or belief that any anomalous spacecraft behavior had occurred. As per design, the ESR event resulted in a reconfiguration of the gyros. Gyro A replaced Gyro C as the roll gyro used for the ESR thruster-based control mode, while Gyro B remained configured as the fault detection gyro. The error in Gyro B's gain was discovered and corrected, but the Gyro A despun status was not identified.

After transitioning to the ISA mode as part of the normal ESR recovery sequence, the attitude control system began integrating the gyro drift rate bias associated with the still despun Gyro A. After 15 minutes, this resulted in roll thruster firings intended to null the apparent (but non-existent) roll attitude error. In less than one minute, the roll rate was sufficiently high to trigger the Gyro B based fault detection once again, resulting in ESR-6 at 10:35 PM EDT (02:35 UT), June 24, 1998.

Although the spacecraft remained Sun-pointing within nominal limits and was therefore in a power-positive and thermally-safe attitude, the state of the spacecraft was precarious at this point in time. It had an anomalous roll rate and was depending on a deactivated gyro for roll control in both ESR and ISA modes. The personnel on the ground were not aware of either of these facts at that time. Gyro C was correctly configured to the ACU since the reconfiguration at ESR-5. Gyro B was active and on-line for fault detection, and it was correctly measuring the anomalous roll rate. A rapid decision was made that Gyro B was faulty because its output disagreed with the rate indicated by Gyro A. This decision led to the commanding off of Gyro B.

During ESR-6 recovery, Ground Operations commanded the spacecraft to ISA mode. In ISA, the attitude control system resumed firing roll thrusters in an attempt to null the attitude error associated with the electrical rate bias term of the despun Gyro A. Gyro B and the associated fault detection were now inactive. The increasing roll rate eventually resulted in pitch and yaw Sun-pointing errors that exceeded a prescribed limit of five degrees, resulting in ESR-7 at 12:38 AM EDT (04:38 UT), June 25, 1998. Due to the gyroscopic cross-coupling torques caused by pitch and yaw thruster firings, and the absence of true roll rate indications, the ESR controller was no longer stable, and the spacecraft attitude diverged. **The incorrect diagnosis of a Gyro B fault and the subsequent ground response to this diagnosis ultimately resulted in loss of attitude control, subsequent loss of telemetry, and loss of power and thermal control.** Loss of telemetry occurred at 12:43:56 AM EDT (04:43:56 UT), June 25, 1998. It can not be determined whether this loss was a consequence of insufficient power or a loss of communication link caused by spacecraft attitude.

At any time during the over five hour emergency situation, the verification of the spinning status of Gyro A would have precluded the mishap.

For further information, a more detailed timeline summarizing the sequence of events leading up to the mishap is provided in Appendix C. A detailed fault tree analysis supporting the above scenario and the Board's conclusions has been performed by MMS and is on file.

FACTORS INDIRECTLY CONTRIBUTING TO FAILURE

In addition to the Board findings that the SOHO mishap was due directly to operational errors, a failure to adequately monitor spacecraft status, and an erroneous decision which disabled part of the on-board autonomous failure detection, the Board has also identified a number of contributory factors. The failure tree developed by the Board that identifies the primary as well as indirect contributory causes is contained in Appendix D. The indirect contributory factors are discussed below under four broad categories: Ground Procedures, Procedure Implementation, Management Structure and Process, and Ground System.

A. GROUND PROCEDURES

1. Failure to control change

The Flight Operations Team (FOT) modified flight-demonstrated ground operations procedures (predefined stored sequences of ground generated commands) as a part of the ISTP Ground System re-engineering effort to reduce operations cost for the SOHO extended mission, to streamline the operations to minimize science downtime, and to conserve gyro life. Though some of these modifications were made at the request of the SOHO Science Team, they were not necessarily driven by any specific requirement changes. The procedure modifications appear to have not been adequately controlled by ATSC configuration board, properly documented, nor reviewed and approved by ESA and/or NASA. The verification process was accomplished using a NASA computer-based simulator. There was no code walk-through as well as no independent review either by ESA, MMS, or an entity directly involved in the change implementation. No hard copy of the command procedure set exists, and the latest versions are stored electronically without adequate notification of procedure modifications.

A more complete history of a critical procedure modification directly contributing to the SOHO Mission Interruption is provided in Appendix E.

It is noted that the previous ESR's 3 and 4 had also been triggered by ground software problems and that a recommended comprehensive review of the software and procedures had not been implemented due to higher priorities given to other tasks of the FOT.

2. Failure to perform risk analysis of a modified procedure set

As stated above, multiple ground operations procedures were modified. Each change was considered separately, and there appears to have been little evaluation performed to determine whether any of the modifications had system reliability or contingency mode implications; or whether the use of this modified procedure set should have been accompanied with operational constraints.

3. Failure to communicate change

The functional content of an operational procedure, A_CONFIG_N, was modified without updating the procedure name and without communicating either to ESA or MMS the fact that there had been a functional change. Consequently, a cursory review of a ground operations script of procedure names, rather than a review of the commands generated by the procedure, contributed to the initiation of a calamitous sequence of events. The A_CONFIG_N procedure had been developed to simply reconfigure the three roll gyros after calibration; however, the procedure had also been modified to provide options to perform gyro spin down.

The SOHO autonomous safe mode requires the use of Gyro A for roll control. Accordingly, any procedure that spins down Gyro A must also enable a software flag in the on-board computer to respin Gyro A whenever the safe mode is triggered. Unfortunately, this software enable command had not been included as part of the modification to A_CONFIG_N due to a lack of system knowledge of the person who modified the procedure. Coupled with the inadequate change review process described above and the fact that the enable command was missing, the likely impact of not enabling Gyro A in this procedure was not recognized. Because the functionality of A_CONFIG_N had changed and the change had not been properly communicated, a casual review of a script comprised of procedure names would not have indicated that Gyro A had been spun down. Previously, the procedure IRU-REST had been used to spin down the gyros; this procedure would have restored the software enable before completion.

B. PROCEDURE IMPLEMENTATION

4. Failure to properly respect autonomous Safe Mode triggers

SOHO had been designed to autonomously enter a simple, independent safe mode in response to a variety of on-board detected anomalous conditions. This mode was intended to safe the spacecraft, and to allow the FOT and cognizant engineering staff sufficient time to understand and rectify problems before putting the spacecraft at risk by re-commanding normal mode operations. The operations team did not take advantage of the 48 hour minimum safe mode design, and initiated recovery almost immediately after each of the two emergency safe mode entries that occurred prior to the loss of the spacecraft. The operations team did not appear to respect the seriousness of the safe mode entries. It is to be noted that in March 1998, a similar shortcut in the recovery from ESR 3 led to ESR 4. Recovery had been effected without long-term spacecraft impact, thus developing a false sense of confidence in the operations team in the ability to recover from an ESR.

5. Failure to follow the operations script; failure to evaluate primary and ancillary data

Real time data becomes limited because an autonomous data format change occurs whenever the spacecraft enters safe mode. However, the spacecraft status immediately preceding a safe mode trigger could have been determined

by viewing the history tape that was generated prior to an anomaly. In addition, SOHO was designed to store, within its on-board computer for diagnostic purposes, the last three telemetry frames that preceded a safe mode entry. The operations script specifically states that the Gyro A is to be spinning upon entry into safe mode and instructs the operator to evaluate the three telemetry frames that had been stored prior to the anomaly before proceeding toward recovery.

Neither the confirmation of Gyro A state nor the evaluation of the three previous telemetry frames was performed. These omissions resulted in a failure to notice that Gyro A was not spinning - a state which rendered the safe mode unstable. This ultimately resulted in a misinterpretation of Gyro B data, and eventually caused the loss of a SOHO safety net.

It was only later realized that three of four battery discharge regulators were disconnected from the bus. In fact, analysis indicated that this condition had occurred several months prior and no one had recognized this change in the spacecraft configuration. This limited access to battery discharge current when the spacecraft needed it for control. There is no evidence that this has been a contributing or aggravating factor to the loss of the attitude; however, this inappropriate power configuration may have limited the duration of the telemetry transmission in the minutes after the loss of the attitude of the spacecraft.

6. Failure to question telemetry discrepancies

During the final hours prior to the loss of SOHO, it was observed that Gyro A indicated zero rate while Gyro B indicated a variable non-zero rate. Rather than corroborating these data discrepancies with other telemetry points from real time or history data, Gyro B was assumed to be in error. As an example, the lack of correlation between the thruster firing activity and variations in Sun sensor data and the continued zero rate error indication of Gyro A went unnoticed. The MMS engineer and the FOT mission manager concluded that Gyro B had to be spun down. This action eliminated the SOHO high roll rate autonomous safety net. Standard procedure requires a Materials Review Board (MRB) before such a critical action (a declared key component failure) can be taken. The MRB would have provided a formal process for senior management and engineering staff to review and decide on the risks involved. An MRB was not convened.

C. MANAGEMENT STRUCTURE AND PROCESS

7. Failure to recognize risk caused by operations team overload

It appeared that the FOT's overly aggressive operations plan, scheduled to begin on the morning of June 24 and run through June 29, was primarily driven by DSN scheduling and science planning. This ambitious plan included the calibration of three gyros and a momentum management event performed in a compressed timeline never attempted previously, a yaw maneuver that exceeded previously established positional offset bias constraints, a 24-hour roll maneuver, phased reaction wheel maintenance, momentum management, a station keeping maneuver, and the loading of a star sensor software patch. The plan was to execute this timeline using the SOHO core team with no augmented staff. The planned activities were intensive and there was no contingency time built into the schedule.

Operations were being conducted from an integrated ISTP Mission Operations Center (IMOC), which was still under test. An IMOC-related ground system software change caused a reaction wheel to be commanded to an incorrect speed. After the "streamlined" procedure error triggered a safe mode entry for the first time that day (ESR-5), the FOT retreated to the old SOHO control center. Due to the compressed nature of the gyro calibration and the momentum management, neither the ESA technical support manager, the MMS engineer, nor the FOT had the time available to analyze the results of the gyro calibrations. Therefore, valuable information that should have been factored into the recovery scenario was not taken into consideration.

The second safe mode trigger (ESR-6) occurred while the MMS engineer was trouble shooting discrepancies between NASA and ESA simulator results required for the upcoming science maneuver, and responding to a science investigator's need to service his instrument. These caused a distraction; yet no one directed that the plan should be aborted until all of the problems could be better understood. Clearly in their haste to continue, inappropriate decisions were made, an autonomous safety net was disabled, and the spacecraft was inappropriately commanded leading to the loss of communications with the SOHO spacecraft. Ironically, the motivation for the aggressive flight operations plan was to restore the spacecraft to perform science as quickly as possible.

8. Failure to recognize shortcomings in implementation of ESA/NASA agreements

The MOU states that "ESA retains ownership of the spacecraft ... and is responsible for the technical integrity and safety of the spacecraft and science instrumentation at all times".

At a lower level, the SOHO ESA/NASA Mission Management Plan further states that following in-orbit commissioning, mission management authority would be transferred from the ESA Project Manager to the ESA Project Scientist, resident at GSFC. The ESA Project Scientist would be supported by an ESA technical support manager, also resident at GSFC, who would have access to additional ESA and MMS technical support. In practice, after the spacecraft's first year in orbit, the support team was typically comprised of the ESA technical support manager, one MMS

engineer, and occasionally additional engineers from Europe for important maneuvers. The level of support is judged not commensurate with the intent that ESA retain full responsibility for the health and safety of the spacecraft. They were understaffed to perform this function in other than routine situations.

The Mission Management Plan requires that the NASA project operations director be responsible for programmatic matters, to provide "overall technical direction" to the FOT, and to "interface" with the ESA technical support manager. The position has been descoped over time by NASA from a dedicated individual during launch and commissioning, to one NASA individual expending less than 10% of his time tracking SOHO operations. In addition, this position changed hands five times throughout the life of the mission; the most recent change occurring three weeks prior to the event.

A direct result of this operational structure was the lack of clear leadership in the handling of contingency situations.

9. Emphasis on science return at expense of spacecraft safety

The transfer of management authority to the SOHO Project Scientist resident at GSFC left no manager, either from NASA or ESA, as the clear champion of spacecraft health and safety. Rather, the transition encouraged management decisions that were intended to maximize science return without properly emphasizing spacecraft risk. This is evident by the fact that, after ESR-5, the attention of one of the key technical experts present was diverted from the spacecraft emergency situation by a request to uplink commands to an instrument to maintain thermal balance. The main focus of the group was the return to the challenging timeline.

10. Over-reliance of flight operations team on ESA and MMS representatives

The FOT was not sufficiently versed regarding details of the spacecraft design and its idiosyncrasies. There were significant training opportunities for the original FOT staff; however as turnover occurred, training opportunities became more limited. The Board was told that video taped training sessions could have augmented this training, but that there was no time to take advantage of this type of additional training sessions. Accordingly, the FOT placed a high reliance on ESA and MMS representatives who were quite knowledgeable on the spacecraft design. However, there were only two of them, and neither was versed in TSTOL, the computer language that was used to define the procedural predefined sequences of ground generated commands. Consequently, the level of procedure verification that the ESA and MMS personnel could provide was limited.

11. Dilution of observatory engineering support

The technically skilled FOT members' ability to support observatory off-line analysis and concentrate on real-time health and safety monitoring was compromised by having to support operational aspects within the Control Center in addition to trouble shooting problems encountered with Control Center interfacing organizations. In addition some FOT key members were obliged to concurrently support on-going ISTP re-engineering activities.

These conditions were worsened by the ATSC decision to eliminate the Lead Engineer position and distribute Lead Engineer responsibilities across Observatory Engineers and the Flight Operations Manager. The FOT was left without any clear management focus and with decreasing flexibility in the allocation and execution of work assignments.

D. GROUND SYSTEMS

12. Failure to resolve a critical deficiency report in a timely manner

SOHO was designed to store within its on-board-computer, for diagnostic purposes, the last three telemetry frames that precede a safe mode entry. A deficiency report that was written in 1994, stating that the SOHO control center was unable to display this data in a convenient (user friendly) format, was never resolved. Ironically, this feature had been included in the newly configured IMOC; and although the FOT had been resident in the IMOC when the first safe mode entry was triggered (ESR-5), the frozen data was not displayed. Had it been displayed, it would have become obvious that Gyro-A was not spinning, and the sequence of events that followed should have been avoided.

13. Failure to validate the planned sequence of events in advance

As part of the planning of the ambitious timeline for the week of June 24, the NASA simulator was unable to independently substantiate the planned sequence of events. In fact, the NASA simulation results indicated that problems existed in the planned timeline. Analysis of the differing simulation results (ESA vs. NASA simulator runs) was continuing as the timeline execution was in process. This, in itself, was an indirect factor in the failure scenario since the technical support staff were distracted by the on-going simulation evaluation rather than focusing on the ESR recovery efforts.

It is further noted that the simulator had not been maintained with all on-board software changes that had been implemented on the spacecraft.

-

RECOMMENDATIONS

The Board strongly recommends that the two Agencies proceed immediately with a comprehensive review of SOHO operations, addressing issues in the ground procedures, procedure implementation, management structure and process, and ground systems. This review process should be completed and process improvements initiated prior to the resumption of SOHO normal operations. The recommendations are described below in detail.

A. GROUND PROCEDURES

1. An ESA and NASA review of the process for SOHO operational procedure change should be implemented forthwith. The review should critically assess the process from beginning to end. The review should include matters such as who can initiate a change, who agrees it should be made, how is the modification process monitored, how is it validated, how is it introduced into operations, how it is signed-off, how are the users of the procedure informed of the change, and how are users trained on the new version.
2. All SOHO procedures modified since launch should be identified and subjected to a thorough review of the changes made and their verification and validation status. The review should be led by ESA and supported by MMS, NASA, and the FOT. This review should be completed before the resumption of routine operations. If there is any doubt about a procedure, it should be re-validated.

B. PROCEDURE IMPLEMENTATION

1. NASA should perform an immediate comprehensive audit of all ISTP on-going flight operations activities to assess conformance to contractual requirements addressing areas such as leadership, configuration management, roles/responsibilities, anomaly handling, and general procedure implementation and validation. The activities pertinent to SOHO should include ESA in the review.
2. ESA and NASA should review the decision authority for real-time divergence from agreed upon ground or spacecraft procedures. In the event that a problem is encountered during any procedure execution, the decision authority for the subsequent action must be clearly defined. Spacecraft safety must never be compromised.
3. It is critical that NASA should review the relevance of selected metrics to determine adequacy for contractor performance evaluation.

C. MANAGEMENT STRUCTURE AND PROCESS

1. ESA and NASA should review the allocation of their responsibilities for the operation of the SOHO mission, as defined in the STSP MOU, Program Plan, and SOHO Mission Management Plan. Assessment should be made as to how these responsibilities have been undertaken by both parties. Changes should be proposed and implemented where appropriate. In particular, ESA's responsibilities for the technical integrity and safety of the spacecraft and science instrumentation and NASA's responsibilities for Ground Segment infrastructure and the conduct of the mission in accordance with the approved Flight Operations Plan should receive critical focus. This review should be preceded by internal reviews in both Agencies and completed prior to return to normal operations. It is anticipated that the review should result in an improved Mission Management Plan.
2. ESA and NASA should re-assess staffing to ensure it is commensurate with the complexity and criticality of the SOHO mission and consistent with the updated Mission Management Plan. The staffing should be strengthened as required. Surge capability should exist to support non-routine and contingency operations.
3. NASA should perform a risk-based analysis of operations plans to determine the level of insight/oversight appropriate for joint, cooperative, and PI missions with special attention to accountability.

D. GROUND SYSTEMS

1. All operational timelines should be planned and validated well before implementation with proper attention to risk assessment and contingency planning.
2. The operations scripts (the string of procedures used by the FOT) for other than routine science operations should be put under configuration control and any change formally approved by ESA and NASA. Each time such a script is changed, the whole script should be validated.
3. Flight operations should verify response to spacecraft configuration changes and critical commands to ensure proper execution. Flight operations should verify configuration prior to initiating critical spacecraft activity to ensure it is consistent with planned events.
4. ESA/ESOC should lead an independent assessment of the capabilities of the NASA SOHO simulator and provide recommendations for suggested maintenance and enhancements.
5. The FOT should review the current database to ensure that all critical parameters are flagged as out-of-limits (and

preserved) if they violate values as defined in the ESA provided satellite users manual. If possible, automatic monitoring should be extended to all telemetry.

6. An ESA and NASA board should review all outstanding Ground System Problem Reports and the plans to close them.

7. ESA and NASA flight operations personnel should be conversant with both the ESA and NASA systems to the maximum extent possible to form a more synergistic, integrated team.

Appendix A. Assignment Letter

SOHO Mission Interruption Joint ESA/ NASA Investigation Board

1. PURPOSE

This establishes the Solar and Heliospheric Observatory (SOHO) Mission Interruption Joint ESA/ NASA Investigation Board and sets forth its responsibilities, membership and initial operating mandate.

2 . ESTABLISHMENT

a. The SOHO Mission Interruption Joint ESA/ NASA Investigation Board (hereinafter called the Board) is hereby established in the public interest to gather information, analyze, and determine the facts as well as the actual or probable cause(s) of the SOHO mission Interruption . The primary purpose of this board investigation and the subsequent management actions is to identify and affect necessary changes and pursue corrective actions to prevent similar recurrence and thus improve the effectiveness of NASA and ESA operations.

b. The chairpersons of the board will report to the ESA Director of the Scientific Programme and the NASA Associate Administrator of the Office of Space Science.

3. AUTHORITIES AND RESPONSIBILITIES

a. The Board will:

1) Assure the impoundment of property, equipment, and records, to preserve the integrity of existing evidence or data.

Note: Impoundment does not preclude release of information.

General information which would normally be released or had been released previously can continue to be released.

2) The chairpersons shall appoint a spokesperson to communicate externally the daily progress of the Board if deemed appropriate.

3) Obtain and analyze whatever evidence, facts, and opinions it considers relevant by relying upon reports of studies, findings, recommendations, and other actions by ESA/NASA officials and contractors or by conducting inquiries, hearings, tests, and other actions it deems appropriate. In so doing, it may take testimony and achieve statements from witnesses.

4) Pursue the discovery of root cause-effect relationships from which remedial and corrective actions can be derived. The intent is not to place blame but to determine how processes and responsibilities may be clarified and improved and future errors eliminated.

5) Provide an interim report by 10 July 1998 to the ESA Director of Scientific Programme and to the NASA Associate Administrator of the Office of Space Science and a final written report to same by 31 August 1998.

b. The Chairpersons will:

1) Conduct board activities in accordance with any instructions the appointing authorities may invoke. (Note: For NASA, NPD 8621.G and supporting documents will be utilized.)

2) Establish and document, to the extent considered necessary. rules and procedures for the

organization and operation of the board, including any subgroups, and for the format and content of oral or written reports to and by the board.

3) Designate any representatives consultants, experts, liaison officers, or other individuals who may be required to support ft activities of the board

and define the duties and responsibilities of those persons.

4. MEMBERSHIP

The designated Chairpersons, Members of the ESA/ NASA Board and supporting staff are included in Attachment A.

5. MEETINGS

The Chairpersons will arrange for meetings and for such records or minutes of meetings as considered necessary.

6. ADMINISTRATIVE AND OTHER SUPPORT

a. The Director of Goddard Space Flight Center will arrange for office space and other facilities and services that may be requested by the Chairperson or designees. Should a European venue be required, ESA will be responsible for arranging for office space and for other facilities and services that may be requested.

b. All elements of ESA and NASA will cooperate fully with the Board and pr
any records. data, and other administrative or technical support and services that
may be requested.

7. DURATION

The ESA Director of the Scientific Programme and the NASA Associate Administrator of the Office of Space Science will dismiss the board when it has fulfilled its requirements.

8 . CANCELLATION

This appointment letter is automatically canceled 1 year from its effective date unless otherwise specifically extended by the establishing authorities.

Signed by:

ORIGINAL SIGNED BY ORIGINAL SIGNED BY

Dr. R. M. Bonnet - ESA Dr. Wesley T. Huntress - NASA

Attachment A:

Members and supporting staff for the SOHO Mission Interruption Joint ESA/NASA

Investigation Board

Co-Chairman: M. Trella ESA

Co-Chairman: M. Greenfield NASA

Executive Secretary: E. Herring NASA

Members: J. Credland ESA Science Projects

R. Laine ESA Spacecraft Systems

A. Smith ESA Mission Operations

D. Machi NASA/GSFC International Programs

R. Freeman NASA/GSFC Spacecraft Systems

A. Reth NASA/GSFC GN&C

B. Kilpatrick NASA/MSFC Mission Operations

Consultants:

F. Felici ESA SOHO Project

L. Culhane MSSL, University College London Science

M. Bouffard MATRA MARCONI SPACE SOHO Spacecraft

J. Gurman NASA/GSFC Science

J. Leibee NASA/GSFC Mission Operations

K. Walyus NASA/GSFC Mission Operations

H. Hoffman Swales Spacecraft Systems

W. Steigerwald NASA/GSFC Public Affairs

L. Watson NASA/GSFC Legal

C. Mitchell Georgia Tech Human Factors

M. Bay Swales Systems Engineer

Appendix B. Summary of Interviewed Individuals

Name	Organization	Title
Bill Worrall	NASA/GSFC/630.1	Space Science Orbiting Spacecraft Manager
Ron Mahmot	NASA/GSFC/584	Technical Area Owner (TAO), ISTP Re-engineering and ISTP Operational Missions Technical Areas
Keith Walyus	NASA/GSFC/581	Former SOHO Mission Operations Director
Helmut Schweitzer	ESA	SOHO Technical Support Manager
Jean-Phillippe Olive	Matra Marconi Space	SOHO Operations Engineer
Carrie White	ATSC	Former SOHO Flight Operations Manager
Harold Bennefield	ATSC	SOHO Flight Operations Manager; Former SOHO Lead Engineer
Nick Piston	ATSC	SOHO Observatory Engineer
Chris Ginther	ATSC	SOHO Spacecraft Analyst

Appendix C. Sequence of Events

TIMTIME	UT(LOCAL (EDT)	EVENT DESCRIPTION
06/24/98		
22:30	18:30	Noticed RW2 spin rate in error as result of incorrect command data word
22:50	18:50	Manually set command to adjust RW2 spin rate
23:08	19:08	RRAD SET (but FDE was left in high gain for Gyro B = RRAD gyro)
23:16	19:16	ESR-5 triggered by RRAD due to Gyro B in high gain; Data Dropout (the ESR roll controller is enabled but gyro A not spinning)
	19:20	Operations transitioned from IMOC to TPOCC

19:32 2Declared S/C emergency to get DSN 34m support

19:55 2TM resumed in low rate via DSN 34m

(6/25/98

20:12 (Start of ESR-5 data collection

21:05 (Transmitter switch to coherent (induced a short TM gap)

21:25 (Start of ESR-5 recovery

01:21:48 Set drift term ($=-2.83468 \text{ e-6 rad/s}$) and scale factor for Gyro A (ACU-B still in standby)

01:21:52 Anomaly detection set up: RRAD enabled (FDE set to low gain for Gyro B = RRAD gyro)

22:16 (Transition ESR-5-> ISA using gyro A for roll control

22:20 (ACU mode relays to ISA ; gyro A used by ACU but not spinning

22:23 (CAE A check

22:34:26 (Thrusters 6 and 7 (roll) start spinning up the spacecraft

02:22:35:10 **ESR-6 triggered by RRAD due to non-spinning Gyro A used as roll gyro for thruster-based control mode; Data Dropout, TM back 2 min. later**

22:50 (Start of ESR-6 data collection

03:15 23:15 Transmitter switch to coherent (induced a short TM gap)

03:21 23:21 Start of ESR-6 recovery

03:50 23:50 Set drift term for Gyro A ($=-2.83468 \text{ e-6 rad/s}$) (ACU still in standby)

03:53 23:53 Anomaly detection set up: commanded Gyro B OFF and left RRAD disabled; nominal ACU switched to inactive mode

04:11 00:11 Transition ESR-6 -> ISA using Gyro A for roll control

04:20:21 00:20:21 ACU mode relays to ISA; gyro A used by ACU but not spinning

04:21 00:21 CAE A check

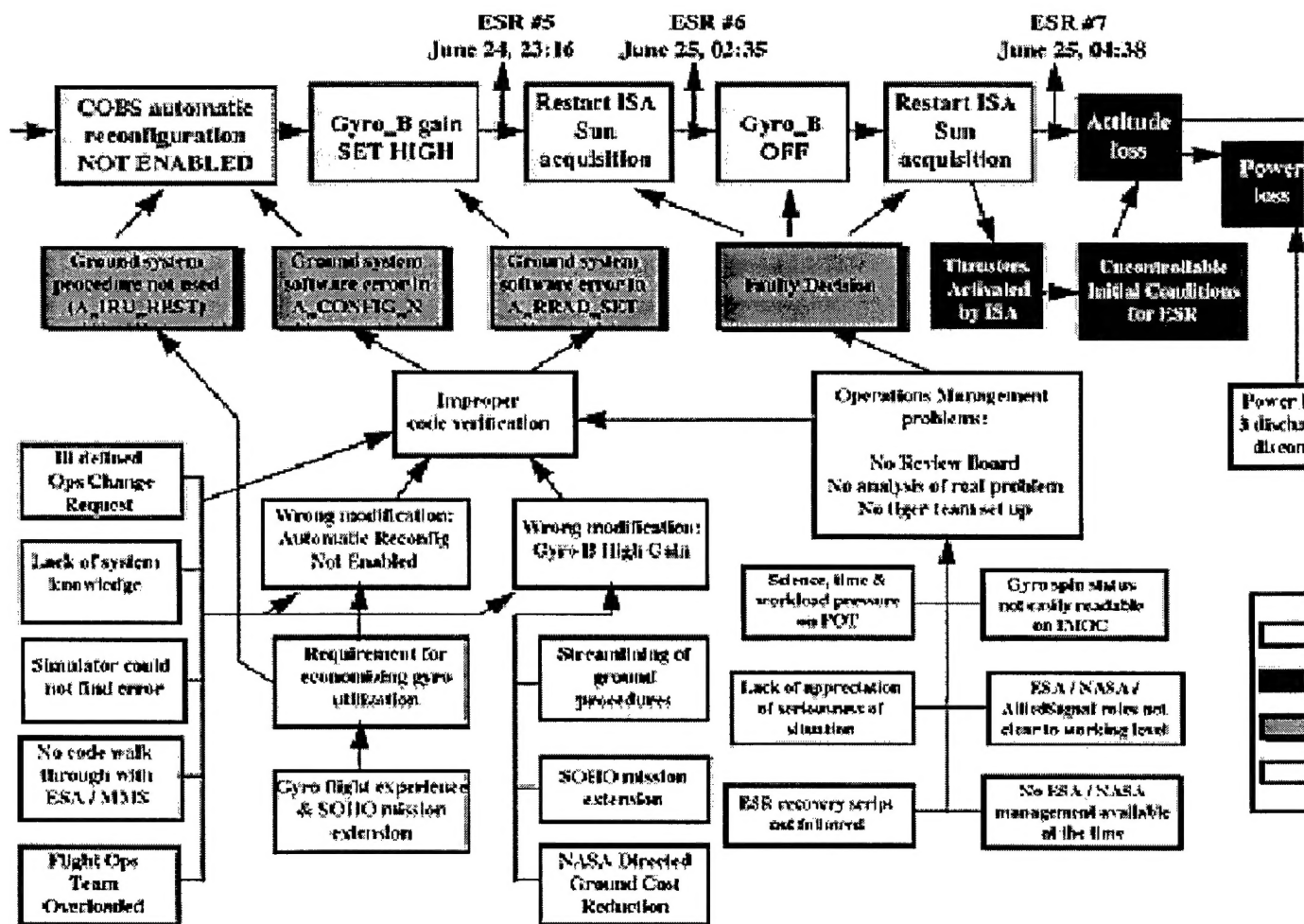
04:35 00:35 Thrusters 6 and 7 (roll) start spinning up the spacecraft

04:38:21 00:38:21 COBS thruster monitoring triggered

00:38:46 **(ESR-7 triggered by fine sun pointing anomaly criteria due to continued reliance on Gyro A; Data Dropout, TM back 2 min. later**

04:43:56 00:43:56 **Lost TM**

Appendix D. SOHO Failure Event Tree



Appendix E. A_CONFIG_N Modification History

Background

A modification in the predefined ground segment sequence of commands called A_CONFIG_N occurred in February 1997. When this modified procedure was used to despin Gyro A, it rendered the SOHO safe mode, Emergency Sun Reacquisition (ESR), unstable because of the absence of roll axis gyro. Correctly configured, the on-board software protects the spacecraft against any single on-board failure or ground segment operational error.

ESR is a "Safe Hold Mode" autonomously entered by the spacecraft in the event of anomalies linked to attitude control. In this mode, a hard-wired control law keeps the spacecraft pointed to the sun with no roll, using thrusters, sun sensors and one roll gyro.

Gyro usage is kept to a minimum because these components are life-limited.

Gyro operations before March 1997

Gyro calibration was performed before each maneuver requiring thruster usage, i.e. every 6 to 8 weeks. This operation was performed 24 hours in advance of the maneuver and gyros were left running from calibration start until end of maneuver, i.e. several days each time.

Use and calibration of gyros basically relies on 5 predefined sequences of commands :

IRU-WAKE Switch-on and spin-up the 3 roll gyros, disable the software function which reactivates gyro A at ESR triggering.

A-CONFIG-1 Configure the gyros for phase 1 of calibration

A-CONFIG-2 Configure the gyros for phase 2 of calibration

A_CONFIG_N Configure the gyros back to their usage mode for maneuvers
IRU-REST Despin and switch-off Gyro B & C, despin and put Gyro A in warm
stand-by and enable software function which respins the stand-
by Gyro A when an ESR is triggered.

Gyro operations after March 1997

Late 1996, after about a year of operations, concern was raised that the gyros were used longer than expected. A European satellite, SAX, had experienced gyro anomalies and the SOHO mission extension was under discussion. It was therefore decided to minimize the usage of gyros and avoid running them when not necessary.

In particular it was decided to despin the gyros between the end of the calibration and the start of the maneuver and to calibrate gyros only every 6 months, not at each maneuver.

As a result of this decision, the 3 command sequences IRU-WAKE, IRU-REST and A_CONFIG_N were modified by the FOT.

Calibrations performed after March 1997

Gyros were calibrated 3 times:

April 1997

September 1997

June 24, 1998

In the first two cases, calibration was effectively performed on the day before the maneuver. The modified IRU-WAKE and IRU-REST sequences were used but not the modified part of A_CONFIG_N.

On June 24, 1998, the plans originally were the same, however they were changed because of a Deep Space Network (DSN) scheduling problem and it was decided to perform gyro calibration just before the wheel momentum management, on the same day.

In such a case it would not have been functionally necessary to despin any of the gyros, but the updated script for the day directed the FOT to despin Gyro A using the option implemented in A_CONFIG_N as a result of the February 1997 modification. This option had never been used before. The modification was not correctly implemented since, unlike IRU-REST, the modified sequence despins Gyro A but does not re-enable the software function that respins it when entering an ESR. This function is mandated for spacecraft safety.

Modification of IRU-WAKE and IRU-REST

These procedures initially turned on (IRU-WAKE) or turned off (IRU-REST) all 3 gyros. As a result of the March 1997 decision, they were modified to be more flexible and allow turning on or off individual gyros as required.

Procedure change was discussed between the FOT and ESA/MMS personnel. Through e-mail exchange, the MMS resident engineer communicated that each time Gyro A is despun, the automatic software function "Gyro Setting at ESR" must be re-enabled.

-

Modification of A_CONFIG_N

The SOHO User's Manual calls for use of IRU-WAKE and IRU-REST for gyro management.

Therefore there was no reason to introduce a new function in A_CONFIG_N to despin gyro A. IRU-REST should have been used all the time.

According to the change record, the modification was completed on February 3, 1997, and a modified procedure A_CONFIG_N was introduced in the operations through a Mission Operations Change Request (MOCR) dated March 3, 1997. An MOCR is internal FOT document not normally distributed to NASA/ESA/MMS.

No one outside the FOT was made aware of this change (i.e., not NASA, ESA, nor MMS personnel).

-

-

ACRONYM LIST

ACU	Attitude Control Unit
ATSC	Allied-Signal Technical Services Corporation
CAE	Control Actuation Electronics
COBS	Central On-Board Software
DSN	Deep Space Network
EDT	Eastern Daylight Time
ESA	European Space Agency
ESOC	European Space Operations Center
ESR	Emergency Sun Reacquisition
ESTEC	European Space Research and Technology Center
FDE	Fault Detection Electronics
FOT	Flight Operations Team
GSFC	Goddard Space Flight Center
IMOC	Integrated Mission Operations Center
IRU	Inertial Reference Unit
ISA	Initial Sun Acquisition
ISTP	International Solar & Terrestrial Program
MMS	Matra Marconi Space
MOCR	Mission Operations Change Request
NASA	National Aeronautics and Space Administration
PI	Principal Investigator
POCC	Payload Operations Control Center
REST	Restore
RRAD	Roll Rate Anomaly Detector
RW	Reaction Wheel
S/C	Spacecraft
SOHO	SOLar and Heliospheric Observatory
TM	Telemetry
TPOCC	Transportable POCC
TSTOL	TPOCC System Test & Operations Language
URL	Universal Resource Locator
XMM	X-ray Multi Mirror